Searching PAJ

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-117661
(43)Date of publication of application : 27.04.2001

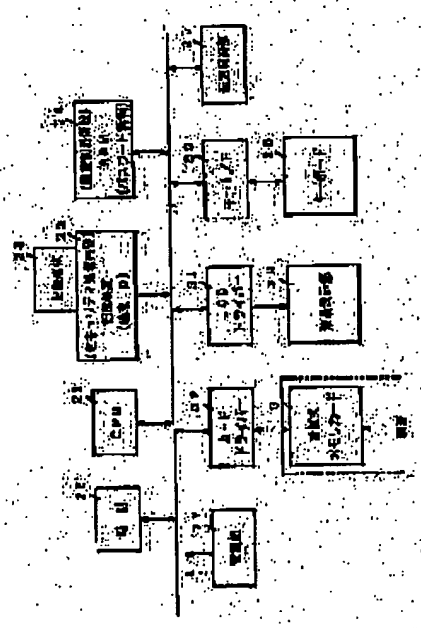
(51)Int.Cl. G06F 1/00
G06F 15/02
G06K 17/00
G09C 1/00
H04L 9/32

(21)Application number : 11-293095
(22)Date of filing : 15.10.1999

(71)Applicant : CASIO COMPUT CO LTD
(72)Inventor : MORIKAWA SHIGENORI
IMADA MASAYUKI

(54) PORTABLE INFORMATION TERMINAL EQUIPMENT AND PROGRAM RECORDING MEDIUM FOR THE SAME

(57)Abstract:
PROBLEM TO BE SOLVED: To surely prevent leakage of memory contents by deciding that possibility that a portable terminal or a portable recording medium is lost or stolen is high, when identification information specific to a user for limiting the user is repeatedly erroneously inputted.
SOLUTION: A CPU 21 compares an inputted password with a set password in advance and determines whether they match. As a result, each time it is determined that they do not match, the number of times when they are do not match is counted as the number of times when the input of the password fails, and whether or not the counted number of times when the input of the password fails is beyond the preliminarily set number of times, when the input of the password is limited is determined, and if the judged result is 'YES', application/data in a storage device 22 or an attachable/detachable memory card 3 can be deleted.



LEGAL STATUS

[Date of request for examination] 16.12.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－117661
（P2001－117661A）
(43)公開日　平成13年４月27日(2001.4.27)

(51)Int.Cl.⁷	識別記号	FI		テーマコード（参考）
G06F 1/00	370	G06F 1/00	370E	5B019
15/02	360	15/02	360Z	5B058
			360B	5J104
G06K 17/00		G06K 17/00	T	9A001
G09C 1/00	640	G09C 1/00	640D	

審査請求　未請求　請求項の数８　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願平11－293095

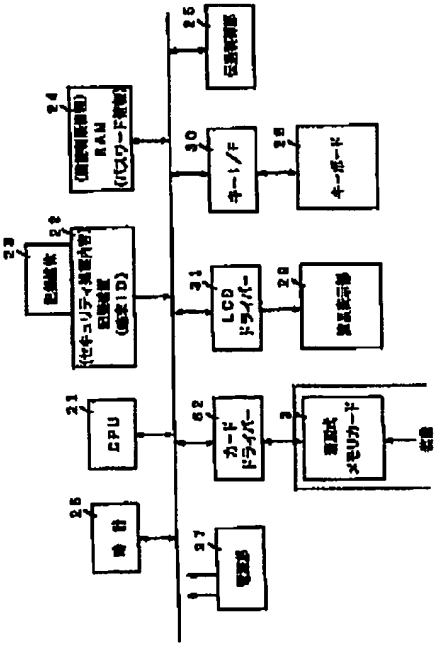
(22)出願日　平成11年10月15日(1999.10.15)

(71)出願人　000001443
カシオ計算機株式会社
東京都渋谷区本町１丁目６番２号
(72)発明者　森川　章則
東京都東大和市桜が丘２丁目229番地　カシオ計算機株式会社東京事業所内
(72)発明者　今田　雅幸
東京都東大和市桜が丘２丁目229番地　カシオ計算機株式会社東京事業所内
(74)代理人　100073221
弁理士　花輪　義男

最終頁に続く

(54)【発明の名称】　携帯型情報端末装置およびそのプログラム記録媒体

(57)【要約】
【課題】利用者を制限する利用者固有の識別情報の入力が繰り返し誤った場合に、携帯端末や可搬型記録媒体を紛失したり、盗難された可能性が高いと判断してメモリ内容の漏洩を確実に防止する。
【解決手段】ＣＰＵ21は、入力されたパスワードと予め設定されている設定パスワードとを比較して両者が一致するかを判別する。その結果、不一致が判別される毎に、その不一致回数をパスワードの入力失敗回数として計数すると共に、計数された入力失敗回数が予め設定されている入力限度回数を超えたかを判別し、入力限度回数を超えている場合には、記憶装置22内や着脱式メモリカード３内のアプリケーション／データを消去する。



【特許請求の範囲】

【請求項１】利用者を制限する利用者固有の識別情報を記憶する識別情報記憶手段と、入力された識別情報と前記識別情報記憶手段に記憶されている識別情報とを比較して両者が一致するかを判別する１の判別手段と、この判別手段によって不一致が判別される毎に、その不一致回数を識別情報の入力失敗回数として計数する計数手段と、この計数手段によって計数された入力失敗回数が予め設定されている入力限度回数を超えたかを判別する第２の判別手段と、この第２の判別手段によって入力失敗回数が入力限度回数を超えたことが判別された場合に、メモリ内容の漏洩を防ぐためのセキュリティ処理を強制実行するセキュリティ処理実行手段とを具備したことを特徴とする携帯型情報端末装置。

【請求項２】前記セキュリティ処理実行手段は、メモリ内容の漏洩を防ぐためのセキュリティ処理として、そのメモリに対するアクセスプロテクトあるいはその記憶内容を消去するセキュリティ処理を強制実行するようにしたことを特徴とする請求項1記載の携帯型情報端末装置。

【請求項３】前記セキュリティ処理実行手段は、アプリケーションソフトを実行不可能な状態にセットするアプリケーション実行不能処理、表示画面を表示不可能な状態にセットする表示不能処理、電源投入を不可能な状態にセットする電源投入不能処理、キー入力を不可能な状態にセットするキー入力不能処理のうち、少なくともそのいずれかをセキュリティ処理として実行するようにしたことを特徴とする請求項１記載の携帯型情報端末装置。

【請求項４】端末装置本体に対して着脱可能に装着される可搬型記録媒体内に前記利用者を制限する利用者固有の識別情報を記憶する識別情報記憶手段を設け、前記第１の判別手段は、前記可搬型記録媒体内に記憶されている識別情報を取得し、この識別情報と入力された識別情報とを比較して両者が一致するかを判別するようにしたことを特徴とする請求項１記載の携帯型情報端末装置。

【請求項５】利用者を制限する利用者固有の識別情報を記憶する識別情報記憶手段と、入力された識別情報と前記識別情報記憶手段に記憶されている識別情報とを比較して両者が一致するかを判別する第１の判別手段と、この判別手段によって不一致が判別される毎に、その不一致度合いに応じてそれらの類似度を認識する認識手段と、前記第１の判別手段によって不一致が判別される毎に、前記認識手段によって認識された類似度別に、その不一致回数を識別情報の入力失敗回数として計数する計数手段と、この計数手段によって計数された類似度別の入力失敗回数が予め類似度別に設定されている入力限度回数を超えたかを判別する第２の判別手段と、前記類似度別の入力失敗回数が予め類似度別に設定されている入力限度回数を超えたことが前記第２の判別手段によって判別された場合に、当該類似度に応じたセキュリティ処理を実行するセキュリティ処理実行手段とを具備したことを特徴とする携帯型情報端末装置。

【請求項６】前記類似度別に予め設定されている設定回数として、前記類似度が高いほど大きな値を設定しておくことにより、類似度が高いほど識別情報を再入力することができる入力可能回数を増やすようにしたことを特徴とする請求項５記載の携帯型情報端末装置。

【請求項７】コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、利用者を制限する利用者固有の識別情報が入力された際に、入力された識別情報と予め記憶されている識別情報とを比較して両者が一致するかを判別させるコンピュータが読み取り可能なプログラムコードと、不一致が判別される毎に、その不一致回数を識別情報の入力失敗回数として計数させるコンピュータが読み取り可能なプログラムコードと、計数された入力失敗回数が予め設定されている入力限度回数を超えたかを判別させるコンピュータが読み取り可能なプログラムコードと、入力失敗回数が入力限度回数を超えたことが判別された場合に、メモリ内容の漏洩を防ぐためのセキュリティ処理を強制実行させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【請求項８】コンピュータが読み取り可能なプログラムコードを有する記録媒体であって、利用者を制限する利用者固有の識別情報が入力された際に、入力された識別情報と予め記憶されている識別情報とを比較して両者が一致するかを判別させるコンピュータが読み取り可能なプログラムコードと、不一致が判別される毎に、その不一致度合いに応じてそれらの類似度を認識させるコンピュータが読み取り可能なプログラムコードと、不一致が判別される毎に、前記認識された類似度別に、その不一致回数を識別情報の入力失敗回数として計数させるコンピュータが読み取り可能なプログラムコードと、計数された類似度別の入力失敗回数が予め類似度別に設定されている入力限度回数を超えたかを判別させるコンピュータが読み取り可能なプログラムコードと、
前記類似度別の入力失敗回数が予め類似度別に設定されている入力限度回数を超えたことが判別された場合に、当該類似度に応じたセキュリティ処理を実行させるコンピュータが読み取り可能なプログラムコードとを有する記録媒体。

【発明の詳細な説明】

【０００１】この発明は、セキュリティ管理機能を備えた携帯型情報端末装置およびそのプログラム記録媒体に関する。

【０００２】

【従来の技術】近年、営業担当者が携帯型情報端末装置を持参して日常の営業活動を行う場合において、この端末本体にフロッピディスク等の可搬型記録媒体を装着し、

営業担当者は外出先でその記憶内容をアクセスして表示出力させたり、データの書き込み等を行っている。ところで、一般に携帯型情報端末装置は、個人専用機として、また、外出先で使用するという関係上、デスクトップ型のパーソナルコンピュータ等で実施している厳密なセキュリティ管理よりも、操作の簡素化、迅速性等の操作環境を重視している。

【０００３】

【発明が解決しようとする課題】しかしながら、携帯型情報端末装置は、外出先に持ち運んで使用する関係上、可搬型記録媒体や携帯型情報端末装置自体を外出先で紛失したり、盗難される危険性があり、可搬型記録媒体や内蔵メモリ内に機密性が高い重要な企業情報や個人情報が格納されている場合には、紛失や盗難によって重要情報が他人に漏洩されるおそれがあった。第１の発明の課題は、利用者を制限する利用者固有の識別情報の入力が繰り返し誤った場合に、携帯端末や可搬型記録媒体を紛失したり、盗難された可能性が高いと判断してメモリ内容の漏洩を確実に防止できるようにすることである。第２の発明の課題は、利用者を制限する利用者固有の識別情報の入力が繰り返し誤った場合に、正規の利用者が識別情報の一部を忘れてしまったことによる繰り返し入力か、携帯端末や可搬型記録媒体を紛失したり、盗難された可能性が高い場合の繰り返し入力かに応じて適切なセキュリティ管理を実現できるようにすることである。

【０００４】この発明の手段は、次の通りである。請求項第１記載の発明（第１の発明）は、利用者を制限する利用者固有の識別情報を記憶する識別情報記憶手段と、入力された識別情報と前記識別情報記憶手段に記憶されている識別情報とを比較して両者が一致するかを判別する１の判別手段と、この判別手段によって不一致が判別される毎に、その不一致回数を識別情報の入力失敗回数として計数する計数手段と、この計数手段によって計数された入力失敗回数が予め設定されている入力限度回数を超えたかを判別する第２の判別手段と、この第２の判別手段によって入力失敗回数が入力限度回数を超えたことが判別された場合に、メモリ内容の漏洩を防ぐためのセキュリティ処理を強制実行するセキュリティ処理実行手段とを具備するものである。なお、この発明は次のようなものであってもよい。

（１）前記セキュリティ処理実行手段は、メモリ内容の漏洩を防ぐためのセキュリティ処理として、そのメモリに対するアクセスプロテクトあるいはその記憶内容を消去するセキュリティ処理を強制実行する。

（２）前記セキュリティ処理実行手段は、アプリケーションソフトを実行不可能な状態にセットするアプリケーション実行不能処理、表示画面を表示不可能な状態にセットする表示不能処理、電源投入を不可能な状態にセットする電源投入不能処理、キー入力を不可能な状態にセットするキー入力不能処理のうち、少なくともそのいずれかをセキュリティ処理として実行する。

（３）端末装置本体に対して着脱可能に装着される可搬型記録媒体内に前記利用者を制限する利用者固有の識別情報を記憶する識別情報記憶手段を設け、前記第１の判別手段は、前記可搬型記録媒体内に記憶されている識別情報を取得し、この識別情報と入力された識別情報とを比較して両者が一致するかを判別する。請求項１記載の発明においては、入力された識別情報と予め記憶されている識別情報とを比較して両者が一致するかを判別し、その結果、不一致が判別される毎に、その不一致回数を識別情報の入力失敗回数として計数すると共に、計数された入力失敗回数が予め設定されている入力限度回数を超えたかを判別し、入力限度回数を超えている場合には、メモリ内容の漏洩を防ぐためのセキュリティ処理を強制実行する。

したがって、利用者を制限する利用者固有の識別情報の入力が繰り返し誤った場合に、携帯端末や可搬型記録媒体を紛失したり、盗難された可能性が高いと判断してメモリ内容の漏洩を確実に防止することができる。

【０００５】請求項第５記載の発明（第２の発明）は、利用者を制限する利用者固有の識別情報を記憶する識別情報記憶手段と、入力された識別情報と前記識別情報記憶手段に記憶されている識別情報とを比較して両者が一致するかを判別する第１の判別手段と、この判別手段によって不一致が判別される毎に、その不一致度合いに応じてそれらの類似度を認識する認識手段と、前記第１の判別手段によって不一致が判別される毎に、前記認識手段によって認識された類似度別に、その不一致回数を識別情報の入力失敗回数として計数する計数手段と、この計数手段によって計数された類似度別の入力失敗回数が予め類似度別に設定されている入力限度回数を超えたかを判別する第２の判別手段と、前記類似度別の入力失敗回数が予め類似度別に設定されている入力限度回数を超えたことが前記第２の判別手段によって判別された場合に、当該類似度に応じたセキュリティ処理を実行するセキュリティ処理実行手段とを具備するものである。なお、前記類似度別に予め設定されている設定回数として、前記類似度が高いほど大きな値を設定しておくことにより、類似度が高いほど識別情報を再入力することができる入力可能回数を増やすようにしてもよい。請求項５記載の発明においては、入力された識別情報と予め記憶されている識別情報とを比較して両者が一致するかを判別し、その結果、不一致が判別される毎に、その不一致度合いに応じてそれらの類似度を認識すると共に、認識された類似度別に、その不一致回数を識別情報の入力失敗回数として計数し、計数された類似度別の入力失敗回数が予め類似度別に設定されている入力限度回数を超えたことが判別された場合に、当該類似度に応じたセキュリティ処理を実行する。したがって、利用者を制限する利用者固有の識別情報の入力が繰り返し誤った場合

に、正規の利用者が識別情報の一部を忘れてしまったことによる繰り返し入力か、携帯端末や可搬型記録媒体を紛失したり、盗難された可能性が高い場合の繰り返し入力かに応じて適切なセキュリティ管理を実現することができる。

【０００６】

【発明の実施の形態】以下、図１～図６を参照してこの発明の一実施形態を説明する。図１は、サーバ装置側で記憶管理されているアプリケーションソフト／データを持ち運び自在な可搬型記録媒体を介して携帯型情報端末装置に外部提供する端末管理システムを示したもので、このシステムは、例えば、会社組織において会社側に設置させているサーバ装置１と、各営業担当者が持参するモバイル型のクライアント端末（携帯型情報端末装置）２とを有し、各営業担当者は外出先で可搬型記録媒体３内のアプリケーションソフト／データをアクセスしながら営業活動を行い、そして、1日の営業終了時に端末本体から可搬型記録媒体３を抜き取り、それをサーバ装置１側のカードリーダ／ライタ４にセットすると、サーバ装置１はカードリーダ／ライタ４を介して記録媒体３内の営業記録を収集処理するようにしている。

【０００７】可搬型記録媒体３は例えば、コンパクトフラッシュカード（ＣＦカード）等の半導体メモリによって構成されているもので、以下、可搬型記録媒体３を着脱式メモリカードと称する。ここで、図中、各着脱式メモリカード３に付した「＃Ａ」「＃Ｂ」、「＃Ｃ」、‥‥は、端末名称「Ａ」、「Ｂ」、「Ｃ」、‥‥で示される携帯型情報端末装置２に対応付けられた端末対応のカードであることを示している。カードリード／ライタ４は着脱式メモリカード３を複数枚同時にセット可能なもので、複数のカード挿入口を有している。そして、サーバ装置１は着脱式メモリカード３を介して端末装置２側にアプリケーション／データを配布する。

【０００８】すなわち、サーバ装置１は着脱式メモリカード３に書き込む書込対象、つまり、配布対象のアプリケーション／データが任意に指定された際に、ＡＰソフト格納部５、データベース格納部６をアクセスしてそれに対応するアプリケーション／データを呼び出してカードリーダ／ライタ４に与え、それにセットされている１または２以上の着脱式メモリカード３にアプリケーション／データを書き込む。その際、着脱式メモリカード３の媒体番号と、この着脱式メモリカード３を使用することが許可されている携帯型情報端末装置２の端末ＩＤ情報とが着脱式メモリカード３にそれぞれ書き込まれる。なお、図中、ＭＯ１、ＭＯ２、ＭＯ３は、各着脱式メモリカード固有の媒体番号を示し、また、ＩＤ１１、ＩＤ１２、ＩＤ１３は、各端末装置固有の端末ＩＤ情報を示している。図２は、着脱式メモリカード３の記憶内容を示した図で、この例では、媒体番号、端末ＩＤ情報、アプリケーションソフト、データベースとして「ＭＯ１」、「ＩＤ１１」、「α１」、「Ｄ１」が記憶されている他、「パスワード情報」が記憶されている。「パスワード情報」はこの着脱式メモリカード３内のアプリケーションソフト、データベースをアクセスすることが許可されている利用者を制限するものである。

【０００９】図３は、携帯型情報端末装置２の全体構成を示したブロック図である。ＣＰＵ２１は、記憶装置２２内のオペレーティングシステムや着脱式メモリカード３内の各種アプリケーションソフトにしたがってこの携帯型情報端末装置２の全体動作を制御する中央演算処理装置である。記憶装置２２は、オペレーティングシステムや各種アプリケーションソフトの他、データベース、文字フォント等が格納され、磁気的、光学的、半導体メモリ等によって構成されている記録媒体２３やその駆動系を有している。この記録媒体２３はハードディスク等の固定的な媒体若しくは着脱自在に装着可能なＣＤ－ＲＯＭ、フロッピィデスク、ＲＡＭカード、磁気カード等の可搬型の媒体である。また、この記録媒体２３内のプログラムやデータは、必要に応じてＣＰＵ２１の制御によりＲＡＭ（例えば、スタティクＲＡＭ）２４にロードされたり、ＲＡＭ２４内のデータが記録媒体２３にセーブされる。更に、記録媒体はサーバ等の外部機器側に設けられているものであってもよく、ＣＰＵ21は伝送媒体を介してこの記録媒体内のプログラム／データを直接アクセスして使用することもできる。また、ＣＰＵ２１は記録媒体２３内に格納されるその一部あるいは全部を他の機器側から伝送媒体を介して取り込み、記録媒体２３に新規登録あるいは追加登録することもできる。すなわち、コンピュータ通信システムを構成する他の機器から通信回線やケーブル等の有線伝送路あるいは電波、マイクロウエーブ、赤外線等の無線伝送路を介して送信されてきたプログラム／データを伝送制御部２５によって受信して記録媒体２３内にインストールすることができる。更に、プログラム／データはサーバ等の外部機器側で記憶管理されているものであってもよく、ＣＰＵ２１は伝送媒体を介して外部機器側のプログラム／データを直接アクセスして使用することもできる。

【００１０】一方、ＲＡＭ２４には予め設定されているパスワード情報（パスワードやその種類に応じた機能制限情報）が格納されている。図４（Ａ）は、パスワードと機能制限情報（以下、それらを合わせて本体パスワードリストと称する）の内容を示した図で、４種類のパスワードとそれに対応付けられている機能制限情報が設定されている。すなわち、"ＭＹＮＡＭＥ２"、"ＰＲＯＪＥＣＴ５"、"ＧＲＵＯＵＰ３"、"ＧＵＥＳＴ"のパスワードが設定されていると共に、この４種類のパスワードには、パスワードレベルが設定されており、このパスワードレベルに対応付けて機能制限情報が設定されている。なお、パスワードレベルは、それに対応付けられている機能の利用を許可する許可レベルであり、パ

スワードの種類に応じた許可レベルによって利用可能な機能を制限するようにしている。また、図４（Ｂ）は、着脱式メモリカード３に予め設定されているパスワード情報（パスワードやその種類に応じた機能制限情報）を示した図で、１種類パスワードとそのパスワードレベルとそれに対応付けられている機能制限情報が設定されている。

【００１１】上述の本体パスワードリストにおいて、この例では、レベル「１」のパスワード"ＭＹＮＡＭＥ２"に対応する機能制限情報として、"個人用情報の参照を含めて全ての機能を実行可能"が設定されている。また、レベル「２」のパスワード"ＰＲＯＪＥＣＴ５"に対応する機能制限情報として、"個人用情報参照以外の全ての機能を実行可能"が設定され、また、レベル「３」のパスワード"ＧＲＵＯＵＰ３"に対応する機能制限情報として、"グループ限定機能のみ実行可能（着脱式メモリカード３のアクセス不可）"が設定され、更に、レベル「４」のパスワード"ＧＵＥＳＴ"に対応する機能制限情報として、"保存データのアクセス不可"が設定されている。また、着脱式メモリカード３に予め設定されているパスワード情報は、レベル「３」のパスワード"ＭＥＭＯＲＹ６"に対応する機能制限情報として、"着脱式メモリカード３のみアクセス可能）"が設定されている。

【００１２】また、ＲＡＭ２４には図５に示すような「類似パスワードの再入力可能回数情報」、「誤パスワードの再入力可能回数情報」、「類似判定基準文字数」が設定されている。ここで、この実施形態においては、利用者を制限する利用者固有のパスワードの入力が繰り返し誤った場合において、正規の利用者がパスワードの一部を忘れてしまったことによる繰り返し入力か、携帯型情報端末装置２や着脱式メモリカード３を紛失したり、盗難された可能性が高い場合の繰り返し入力かを判定するために、入力されたパスワードと予め設定されているパスワードとの類似度を認識し、その類似度に応じてパスワードの再入力可能回数を変えるようにしている。その際、上述の「類似パスワードの再入力可能回数情報」、「誤パスワードの再入力可能回数情報」、「類似判定基準文字数」が参照される。

【００１３】すなわち、入力されたパスワードと予め設定されているパスワードとの類似度を認識する際、この例では、図５（Ｃ）に示すように、「類似判定基準文字数」として「２文字」が設定されており、２文字以下の入力ミスであれば、正規の利用者がパスワードの一部を忘れてしまったことによる入力と判断し、「類似パスワードの再入力可能回数情報」の設定回数分だけパスワードの入力を受付るが、3文字以上の入力ミスであれば、第三者の不正使用による入力と判断し、「誤パスワードの再入力可能回数情報」の設定回数分だけパスワードの入力を受付るようにしている。この例では、図５（Ａ）に示すように、「類似パスワードの再入力可能回数情報」として「５回」が設定されており、また、図５（Ｂ）に示すように、「誤パスワードの再入力可能回数情報」として「３回」が設定されている。したがって、正規の利用者がパスワードの一部を忘れてしまったことによる繰り返し入力の方が、その設定回数が大きな値となっている。

【００１４】また、図５（Ｄ）は、類似パスワードの入力回数カウンタＣ１を示し、類似パスワードが入力される毎に、その値が更新される。図５（Ｅ）は、誤パスワードの入力回数カウンタＣ２を示し、誤パスワードが入力される毎に、その値が更新される。この場合、入力回数カウンタＣ１によって計数された入力回数と図５（Ａ）の「類似パスワードの再入力可能回数情報」との比較が行われ、また、入力回数カウンタＣ２によって計数された入力回数と図５（Ｂ）の「誤パスワードの再入力可能回数情報」との比較が行われる。これによって両者が一致するまで類似パスワード／誤パスワードの入力を許可するようにしている。なお、入力回数カウンタＣ１、Ｃ２にはその初期値として「１」がセットされている。

【００１５】そして、パスワード入力が「類似パスワードの再入力可能回数」あるいは「誤パスワードの再入力可能回数」を超える場合には、類似パスワード、誤パスワードに応じたセキュリティ処理が強制実行される。このセキュリティ処理情報は、予め記憶装置２２内にその端末ＩＤと共に格納されている。ここで、セキュリティ処理の内容としては、メモリ内容を消去する処理、つまり、記憶装置２２内に格納されている所定のアプリケーションやデータを消去する内蔵メモリ消去処理、着脱式メモリカード３内のアプリケーション／データを消去する着脱式メモリカード消去処理の他、メモリ全体に対するアクセスプロテクト処理、記憶装置２２や着脱式メモリカード３内のアプリケーションを実行不可能な状態にセットするアプリケーション実行不能処理、表示画面を表示不可能な状態にセットする表示不能処理、メイン電源の投入を不可能な状態にセットする電源投入不能処理、キー入力を不可能な状態にセットするキー入力不能処理であり、そのいずれか１つあるいは２以上を組み合わせたセキュリティ処理が実行される。

【００１６】また、携帯型情報端末装置２は、日時情報を得る時計２６、電池を電源とする電源部２７の他、キーボード２８、液晶表示部２９、着脱自在な着脱式メモリカード３と、それに対応するキーインターフェイス３０、ＬＣＤドライバ３１、カードドライバ３２を有している。

【００１７】次に、この第１実施形態における携帯型情報端末装置２の動作を図６に示すフローチャートを参照して説明する。ここで、このフローチャートに記述されている各機能を実現するためのプログラムは、読み取り

可能なプログラムコードの形態で記録媒体２３に格納されており、ＣＰＵ２１はこのプログラムコードにしたがった動作を逐次実行する。また、ＣＰＵ２１は伝送媒体を介して伝送されてきた上述のプログラムコードにしたがった動作を逐次実行することもできる。すなわち、記録媒体の他、伝送媒体を介して外部供給されたプログラム／データを利用してこの実施形態特有の動作を実行することもできる。

【００１８】図６は、電源投入によって実行開始される動作を示したフローチャートである。先ず、各種パラメータを初期化するイニシャライズ処理が行われる（ステップＳ１）。この場合、入力回数カウンタＣ１、Ｃ２にその初期値として「１」がそれぞれセットされる。そして、携帯型情報端末装置の利用開始を宣言するために、端末ＩＤが入力されると（ステップＳ２）、記憶装置２２内に設定されている端末ＩＤと比較して、それが正しいかを判別し（ステップＳ３）、誤入力された場合には、このフローから抜けて、その利用が禁止されるが、正規な端末ＩＤが入力された場合には、パスワードの入力を受け付ける（ステップＳ４）。

【００１９】いま、パスワードが入力されると、図４（Ａ）、（Ｂ）で示した本体パスワードリスト内に設定されているパスワード情報および着脱式メモリカード３内に設定されているパスワード情報のうち、最も許可レベルの高いパスワードを取得し（ステップＳ５）、取得したパスワードと入力パスワードとを比較して両者は完全に一致するかを判別する（ステップＳ６）。ここで、パスワードが１文字だけでも不一致の場合には、本体パスワードリスト・メモリカード内の各種設定パスワード情報のうち、次に許可レベルの高いパスワードを取得する（ステップＳ７）。ここで、パスワードを取得できた場合には（ステップＳ８）、この取得したパスワードと入力されたパスワードとを比較して完全一致するかを判別する（ステップＳ６）。以下、上述したいずれか１つの設定パスワードと完全一致したことが判別されるまで、あるいは全ての設定パスワードにも不一致であることが判別されるまで上述の動作を繰り返す。この結果、いずれかの設定パスワードに一致した場合には、正規なパスワードが入力されたものと判断し、その設定パスワードの許可レベルに対応付けられている機能制限情報に基づいて実行可能な機能を制限して携帯型情報端末装置の利用を開始する（ステップＳ９）。

【００２０】一方、入力パスワードが全ての設定パスワードにも完全一致せずに、全パスワード不一致が検出された場合には、ステップＳ１０に進み、本体パスワードリスト・メモリカード内の各種設定パスワード情報のうち、最も許可レベルの高いパスワードを取得する。そして、取得したパスワードと入力パスワードとを比較して両者の一致部分を認識し、不一致文字数は図５（Ｃ）で示した「類似判定基準文字数」以下かを判別する（ステップＳ１１）。この場合、「類似判定文字数」として「２文字」が設定されているので、3文字以上の不一致であれば、上述の設定パスワードのうち、次に許可レベルの高いパスワードを取得し（ステップＳ１１）、以下、全ての設定パスワードを取得し終わるまで設定パスワードを1つずつ取得しながら、不一致文字数は「類似判定基準文字数」以下かを判別する動作を繰り返す（ステップＳ１１～Ｓ１３）。

【００２１】このようにして入力パスワードと全設定パスワードとを比較した結果、「類似判定基準文字数」以下の設定パスワードが存在しない場合、つまり、入力パスワードが各種設定パスワードと類似しない誤入力パスワードであれば、それに対応する入力回数カウンタＣ２の値に「１」を加算するインクリメント処理を実行する（ステップＳ１４）。そして、更新した入力回数カウンタＣ２の値を読み出し、誤パスワードの入力回数と図５（Ｂ）の「誤パスワードの再入力可能回数情報」とを比較する（ステップＳ１５）。この結果、カウンタ計数値が誤パスワードの再入力可能回数以下であれば、パスワードの再入力を受け付けるためにステップＳ４に戻る。これによってパスワードが再入力された場合、それが誤パスワードであれば、上述と同様に誤パスワードが認識される毎にそれに対応する入力回数カウンタＣ２の値が更新される。

【００２２】これによって、誤パスワードが３回入力されると、誤パスワード対応のカウンタ計数値は「４」となり、誤パスワードの再入力可能回数「３」を超えたことがステップＳ１５で判別される。すると、これを条件としてメモリ内容の漏洩を防ぐためのセキュリティ処理が強制実行される（ステップＳ１６）。この場合のセキュリティ処理としては、メモリ内容を消去する処理を実行するようにしている。つまり、記憶装置２２内に格納されている所定のアプリケーションやデータを消去する内蔵メモリ消去処理や着脱式メモリカード３内のアプリケーション／データを消去する着脱式メモリカード消去処理がメモリ内容の漏洩を防ぐためのセキュリティ処理として実行される。

【００２３】また、上述のステップＳ１１～Ｓ１３の類似パスワード認識処理によって入力パスワードがいずれかの設定パスワードと類似する類似パスワードであれば、それに対応する入力回数カウンタＣ１の値に「１」を加算するインクリメント処理を実行する（ステップＳ１７）。そして、更新した入力回数カウンタＣ１の値を読み出し、類似パスワードの入力回数と図５（Ａ）の「類似パスワードの再入力可能回数情報」とを比較する（ステップＳ１８）。この結果、カウンタ計数値が類似パスワードの再入力可能回数以下であれば、パスワードの再入力を受け付けるためにステップＳ４に戻る。これによってパスワードが再入力された場合、それが類似パスワードであれば、上述と同様に類似パスワードが認識

される毎にそれに対応する入力回数カウンタＣ１の値が更新される。これによって、類似パスワードが５回入力されると、カウンタ計数値は「６」となり、類似パスワードの再入力可能回数「５」を超えたことがステップＳ１８で判別されと、このフローから抜けて、その利用が禁止されるが、類似パスワードの再入力可能回数は、誤パスワードの再入力可能回数より多いので、その再入力によって正規なパスワードが入力された場合には（ステップＳ６）、通常の処理が許可される（ステップＳ９）。

【００２４】以上のように、この一実施形態おいては、利用者を制限するパスワードの入力が繰り返し誤った場合に、その誤った入力回数が予め設定されている入力可能回数を超えた場合には、メモリ内容の漏洩を防ぐためのセキュリティ処理を強制実行するするようにしたから、携帯型情報端末装置２や着脱式メモリカード３を紛失したり、盗難された場合であってもメモリ内容の漏洩を確実に防止できるすることができる。この場合、メモリ内容の漏洩を防ぐためのセキュリティ処理として、そのメモリの記憶内容を消去するようにしたから、重要情報の漏洩防止は確実なものとなる。また、セキュリティ処理としては、メモリ全体に対するアクセスプロテクト処理、アプリケーションソフトを実行不可能な状態にセットするアプリケーション実行不能処理、表示画面を表示不可能な状態にセットする表示不能処理、電源投入を不可能な状態にセットする電源投入不能処理、キー入力を不可能な状態にセットするキー入力不能処理のうち、少なくともそのいずれかを実行するようにすれば、メモリ内容を消去せずに、第三者による不正利用や情報の漏洩を簡単かつ確実に防ぐことができる。

【００２５】また、端末装置本体に対して着脱可能に装着される着脱式メモリカード３内には利用者を制限するパスワード情報を記憶するようにしたから、この着脱式メモリカード３内から取得したパスワード情報と、入力されたパスワードとが一致する場合に限り、着脱式メモリカード３へのアクセスが可能となり、着脱式メモリカード３毎に利用者を制限することができる。また、不一致の場合には着脱式メモリカード３に対してそのメモリ内容の漏洩を防ぐためのセキュリティ処理を強制実行するするようにしたから、着脱式メモリカード３を紛失したり、盗難された場合であっても、情報の漏洩を確実に防ぐことができる。

【００２６】更に、入力されたパスワードと設定パスワード情報とを比較した結果、不一致が判別される毎に、その不一致度合いに応じてそれらの類似度を認識し、類似度別の不一致回数をパスワードの入力失敗回数として計数すると共に、類似度別の入力失敗回数が予め類似度別に設定されている入力可能回数を超えた場合に、当該類似度に応じたセキュリティ処理を実行するようにしたから、パスワードの入力が繰り返し誤った場合に正規の利用者がパスワードの一部を忘れてしまったことによる繰り返し入力か、携帯型情報端末装置２着脱式メモリカード３を紛失したり、盗難された可能性が高い場合の繰り返し入力かに応じて適切なセキュリティ管理を実現することができる。この場合、類似度別に予め設定されている入力可能回数として、類似度が高いほど大きな値を設定するようにしたから、正規の利用者がパスワードの一部を忘れてしまったことによる繰り返し入力の場合には再入力回数が多くなり、携帯型情報端末装置２着脱式メモリカード３を紛失したり、盗難された可能性が高い場合の繰り返し入力の場合には、再入力回数が少なくなるため、パスワードの入力状況に応じて適切なセキュリティ管理を実現することができる。

【００２７】なお、上述した一実施形態においては、端末装置本体に対して着脱可能に装着される可搬型記録媒体として着脱式メモリカード３を例示したが、着脱式メモリカード３に限らず、磁気的、光学的記録媒体あるいはコンパクトフラッシュカード以外のＰＣカードであってもよい。また、携帯型情報端末装置の利用には、キー入力やスイッチ入力等、操作による直接的な利用の他、データ通信によって情報を授受する間接的な利用も含まれる。また、利用者を制限する利用者固有の識別情報として、複数文字のパスワードを入力するようにしたが、利用者の音声を認識する音声認識機能を備えた端末装置においては、音声照合によって本人確認を行うようにしてもよい。

【００２８】

【発明の効果】第１の発明によれば、利用者を制限する利用者固有の識別情報の入力が繰り返し誤った場合に、携帯端末や可搬型記録媒体を紛失したり、盗難された可能性が高いと判断してメモリ内容の漏洩を確実に防止することができる。第２の発明によれば、利用者を制限する利用者固有の識別情報の入力が繰り返し誤った場合に、正規の利用者が識別情報の一部を忘れてしまったことによる繰り返し入力か、携帯端末や可搬型記録媒体を紛失したり、盗難された可能性が高い場合の繰り返し入力かに応じて適切なセキュリティ管理を実現することができる。

【図面の簡単な説明】

【図１】サーバ装置側で記憶管理されているアプリケーションソフト／データを持ち運び自在な可搬型記録媒体を介して携帯型情報端末装置に外部提供する端末管理システムを示したブロック図。

【図２】端末本体に装着される着脱式メモリカード３の記憶内容を示した図。

【図３】携帯型情報端末装置の全体構成を示したブロック図。

【図４】（Ａ）はＲＡＭ２４に格納されている本体パスワードリストの内容を示した図、（Ｂ）は着脱式メモリカード３内格納されているパスワード情報を示した図。

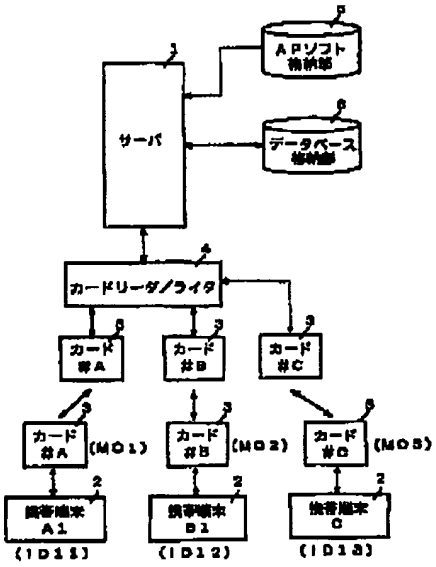
【図５】（Ａ）は設定されている類似パスワードの再入力可能回数情報の内容を例示した図、（Ｂ）は設定されている誤パスワードの再入力可能回数情報の内容を例示した図、（Ｃ）は設定されている類似判断基準文字数情報の内容を例示した図、（Ｄ）は類似パスワードの入力回数カウンタを示した図、（Ｅ）誤パスワードの入力回数カウンタを示した図。

【図６】携帯型情報端末装置２において、メイン電源の投入によって実行開始されるフローチャート。

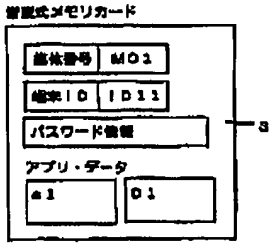
【符号の説明】

２　携帯型情報端末装置
３　着脱式メモリカード
２１　ＣＰＵ
２２　記憶装置
２３　記録媒体
２５　伝送制御部
２８　キーボード
Ｃ１　類似パスワードの入力回数カウンタ
Ｃ２　誤パスワードの入力回数カウンタ

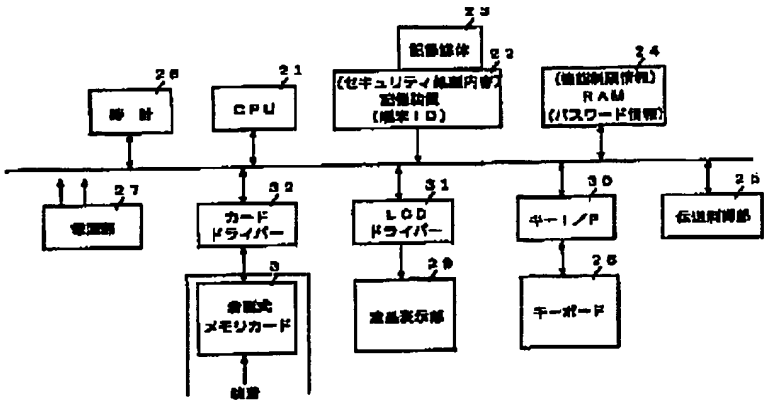
【図１】



【図２】



【図３】



【図４】

本体のパスワードリスト

(A)

パスワード	パスワードレベル	操作制限
"MYPAGE"	レベル１	個人用情報の参照を含めて全ての機能を実行可能
"PROJECT5"	レベル２	個人用情報の参照以外の全ての機能を実行可能
"GROUP3"	レベル４	グループ限定機能のみ実行可能 （着脱式メモリのアクセス不可）
"GUEST"	レベル５	保存データのアクセス不可

着脱式メモリに記憶されたパスワード

(B)

"MEMORY"	レベル３	着脱式メモリのみアクセス可能

【図５】

本体のパスワード

(A) 照合パスワードの再入力可能回数情報：５回

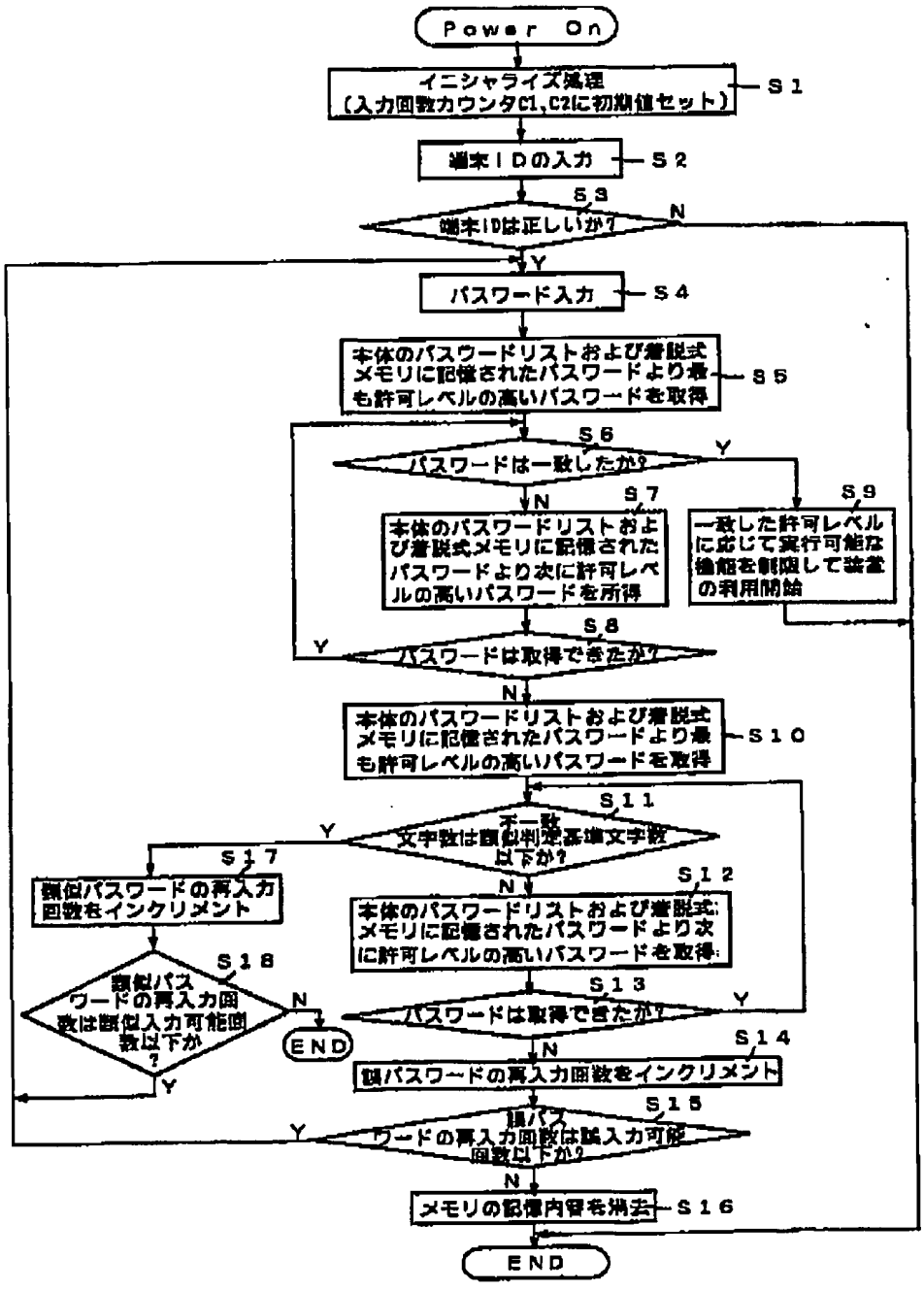
(B) 新パスワードの再入力可能回数情報：３回

(C) 類似判定基準文字数：２文字

(D) 照合パスワード入力回数カウンタ　C1

(E) 新パスワード入力回数カウンタ　C2

【図６】


Power On
イニシャライズ処理
（入力回数カウンタC1、C2に初期値セット）
S1
端末IDの入力
S2
S3
端末IDは正しいか？
N
Y
パスワード入力
S4
本体のパスワードリストおよび着脱式メモリに記憶されたパスワードより最も許可レベルの高いパスワードを取得
S5
S6
パスワードは一致したか？
Y
N
S7
本体のパスワードリストおよび着脱式メモリに記憶されたパスワードより次に許可レベルの高いパスワードを所得
S9
一致した許可レベルに応じて実行可能な機能を制限して装置の利用開始
S8
Y
パスワードは取得できたか？
N
本体のパスワードリストおよび着脱式メモリに記憶されたパスワードより最も許可レベルの高いパスワードを取得
S10
S11
Y
文字数は類似判定基準文字数以下か？
N
S17
類似パスワードの再入力回数をインクリメント
S12
本体のパスワードリストおよび着脱式メモリに記憶されたパスワードより次に許可レベルの高いパスワードを取得
S18
類似パスワードの再入力回数は類似入力可能回数以下か？
N
END
Y
S13
パスワードは取得できたか？
Y
N
S14
類パスワードの再入力回数をインクリメント
S15
類パスワードの再入力回数は類入力可能回数以下か？
Y
N
メモリの記憶内容を消去
S16
END

フロントページの続き

(51)Int.Cl.⁷		識別記号	F I		テーマコード（参考）
G09C	1/00	640	G09C	1/00	640E
H04L	9/32		H04L	9/00	673A

Fターム(参考) 5B019 BC04 EA10 HB05 HB10 HF05
HF10
5B058 CA13 KA01 KA06 KA12 KA33
YA01
5J104 AA12 EA03 KA01 NA05 NA27
NA35 NA41 PA02
9A001 BB03 BB04 BB06 CC05 DD15
JJ12 JZ54 LL03